WHAT IS CLAIMED IS:

1. A user data processor for providing access to a rights controlled data object, the user data processor comprising:

a processing device;

a communications device connected to the processing device and configured to receive an encrypted secure package containing a portion of the rights controlled data object;

a user program running on the processing device, the user program configured to control access to the rights controlled data object;

a user program security module configured to at least partially decrypt the secure package using a user program key; and

a machine key device connected to and associated with the processing device and accessible by the user program, the machine key device configured to restrict the use of the data object to the user data processor using a machine key.

2. The user data processor of Claim 1, wherein the user program is configured to communicate with the machine key device to authenticate the identity of the processing device using the machine key.

3. The user data processor of Claim 2, wherein the processing device is configured to provide rights controlled access to digital video.

4. The user data processor of Claim 1,

wherein the encrypted secure package is encrypted with at least the user program key and the machine key, and

wherein the machine key device is configured to at least partially decrypt the secure package using the machine key.

5. The user data processor of Claim 4, wherein the user program is configured to communicate with the machine key device to authenticate the identity of the processing device using the machine key.

6. The user data processor of Claim 5, wherein the machine key is an asymmetric machine key pair comprising a public machine key and a private machine key.

7. The user data processor of Claim 6, wherein the machine key device is configured to generate the asymmetric machine key pair.

8. The user data processor of Claim 1, further comprising a user key device associated with a user, the user key device detachably connected to the processing device, accessible by the user program, and configured to restrict the use of the data object to the user using a user key.

9. The user data processor of Claim 8,

wherein the user program is configured to communicate with the machine key device to authenticate the identity of the processing device using the machine key, and

wherein the user program is configured to communicate with the user key device to authenticate the identity of the user using the user key.

10. The user data processor of Claim 8,

wherein the encrypted secure package is encrypted with at least the user program key, the machine key, and the user key,

wherein the machine key device is configured to at least partially decrypt the secure package using the machine key, and

wherein the user key device is configured to at least partially decrypt the secure package using the user key.

11. The user data processor of Claim 10,

wherein the user program is configured to communicate with the machine key device to authenticate the identity of the processing device using the machine key, and

wherein the user program is configured to communicate with the user key device to authenticate the identity of the user using the user key.

12. The user data processor of Claim 8, further comprising:

a second security module configured to at least partially decrypt the secure package using a second key; and

a third security module configured to at least partially decrypt the secure package using a third key.

13. The user data processor of Claim 12,

wherein the second security module is configured to communicate with the user key device to authenticate the identity of the processing device using the user key, and

wherein the third security module is configured to communicate with the machine key device to authenticate the identity of the processing device using the machine key.

14. The user data processor of Claim 12,

wherein the second key is a portion of the user key,

wherein the second security module is configured to obtain the second key from the user key device,

wherein the third key is a portion of the machine key, and

wherein the third security module is configured to obtain the third key from the machine key device.

15. The user data processor of Claim 14, wherein the second security module and the third security module are parts of the user program.

16. The user data processor of Claim 1, further comprising a third security module configured to at least partially decrypt the secure package using a third key.

17. The user data processor of Claim 16, wherein the third security module is configured to communicate with the machine key device to authenticate the identity of the processing device using the machine key.

18. The user data processor of Claim 17, wherein the third key is the MAC address of the user data processor.

19. The user data processor of Claim 16,

wherein the third key is a portion of the machine key, and

wherein the third security module is configured to obtain the third key from the machine key device.

20. The user data processor of Claim 19, wherein the third security module is a part of the user program.

21. The user data processor of Claim 1, wherein the user program is implemented in hardware.

22. The user data processor of Claim 1, wherein the user program security module is part of the user program.

23. The user data processor of Claim 1, wherein the processing device is a general purpose computer.

24. The user data processor of Claim 1, wherein the processing device and the machine key device are contained in a single integrated circuit.

25. A method of restricting the use of a data object, the method comprising:

(A) associating a user program key with a user program configured to run on a user data processor;

(B) determining whether the use of the data object is to be restricted to a particular user data processor;

(C) associating a machine key device with the particular user data processor, wherein the machine key device is accessible by the user program, and wherein the machine key device maintains a portion of a machine key; and

(D) encrypting the data object such that decryption requires the user program key and the machine key.

26. The method of Claim 25, further comprising:

(E) providing control elements for controlling the use of the data object through the user program;

(F) transmitting the encrypted data object to the user data processor; and

(G) transmitting the control elements to the user data processor.

27. The method of Claim 26, further comprising:

(H) digitally signing the control elements such that the control elements can be authenticated; and

(I) transmitting the digital signature of the control elements to the user data processor.

28. The method of Claim 27, wherein the machine key is an asymmetric machine key pair comprising a public machine key and a private machine key.

29. The method of Claim 25, wherein (D) comprises:

encrypting the data object with a session key, and

encrypting the session key such that decryption requires the user program key and the machine key.

30. The method of Claim 25, further comprising:

(E) determining whether the use of the data object is to be restricted to a particular user;

(F) associating a user key device with the particular user, wherein the user key device is accessible by the user program, and wherein the user key device maintains a portion of a user key; and

(G) encrypting the data object such that decryption also requires the user key.

31. The method of Claim 30, wherein the user key is an asymmetric user key pair comprising a public user key and a private user key.

32. A method of restricting the use of a rights controlled data object, the method comprising:

(A) associating a user program key with a user program configured to run on a user data processor;

(B) encrypting the data object such that decryption requires the user program key;

(C) determining whether the use of the data object is to be restricted to a particular user data processor;

(D) associating a machine key device with the particular user data processor, wherein the machine key device is accessible by the user program, and wherein the machine key device maintains a portion of a machine key;

(E) creating a machine control element configured to cause the user program to restrict use of the data object to the particular user data processor by authenticating the particular user data processor based upon at least the machine key and by at least communicating with the machine key device; and

(F) transmitting the encrypted data object and the machine control element to the user data processor.

33. The method of Claim 32, further comprising:

(G) including the machine control element in a set of control elements configured to cause the user program to control access to the data object; and

(H) signing the set of control elements,

wherein (F) comprises transmitting the signed set of control elements.

34. The method of Claim 33, further comprising:

(I) determining whether the use of the data object is to be restricted to a particular user;

(J) associating a user key device with the particular user, wherein the user key device is accessible by the user program, and wherein the user key device maintains a portion of a user key;

(K) creating a user control element configured to cause the user program to restrict use of the data object to the particular user by authenticating the particular user based upon at least the user key and by at least communicating with the user key device; and

(L) including the user control element in the set of control elements.

35. The method of Claim 33, wherein the machine key is an asymmetric machine key pair comprising a public machine key and a private machine key.

36. The method of Claim 35, wherein (E) comprises including in the machine control element a digital certificate comprising the public machine key.

37. The method of Claim 32, further comprising

(G) encrypting the data object such that decryption also requires the machine key.

38. A method of restricting the use of a data object, the method comprising:

(A) associating a user program key with a user program configured to run on a user data processor;

(B) determining whether the use of the data object is to be restricted to a particular user data processor;

(C) associating a machine key with the particular user data processor;

(D) encrypting the data object such that decryption requires the user program key and the machine key;

(E) transferring the encrypted data object to the user data processor;

(F) determining whether the data object has been encrypted such that decryption requires the machine key; and

(G) decrypting the data object using the user program key and the machine key.

39. The method of Claim 38, further comprising:

(H) determining whether the use of the data object is to be restricted to a particular user;

(I) associating a user key with the particular user;

(J) encrypting the data object such that decryption also requires the user key;

(K) determining whether the data object has been encrypted such that decryption requires the user key; and

(L) additionally decrypting the data object using the user key.

40. The method of Claim 38,

wherein (D) comprises:

encrypting the data object with a symmetric session key, and

encrypting the symmetric session key such that decryption requires the user program key and the machine key, and

wherein (G) comprises:

decrypting the symmetric session key with the user program key and the machine key, and

decrypting the data object using the decrypted symmetric session key.

41. The method of Claim 40, wherein the user program key is an asymmetric user program key pair comprising a public user program key and a private user program key.

42. The method of Claim 40, wherein the user program key is a symmetric key.

43. The method of Claim 40, wherein the machine key is an asymmetric machine key pair comprising a public machine key and a private machine key.

44. A secure data package for controlling the use of a data object, the package comprising a controlled portion of the data object, the controlled portion encrypted such that decryption requires both a user program key and a machine key, wherein a portion of the user program key is maintained by a user program configured to run on a user data processor to provide controlled access to the data object, wherein the user data processor has a permanently attached machine key device configured to maintain the machine key, and wherein the controlled portion comprises an essential portion of the data object.

45. The secure data package of Claim 44, wherein the controlled portion is additionally encrypted such that decryption requires a user key, wherein the user key is maintained by a user key device associated with a particular user and detachably connected to the processing device.